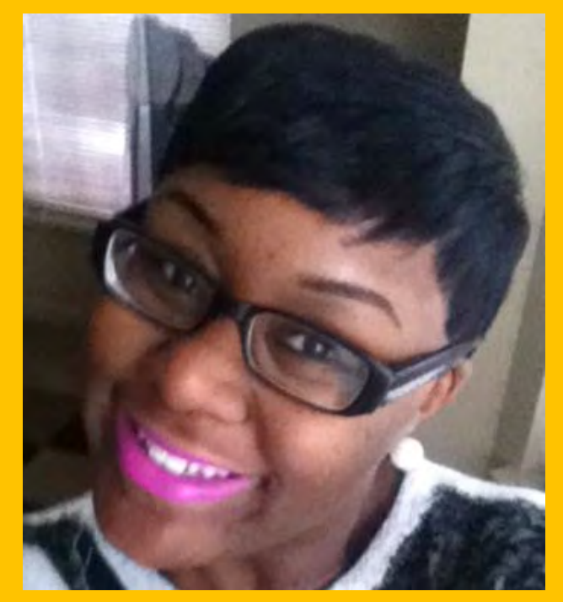
Attacks on WEP Protocol : Brute- Force & FMS Attacks

Valerie Isaac
Allen University
Mentor: Levent Ertaul



Introduction

In Wired Equivalent Privacy (WEP) protocol, all stations share a single secret key. Every time a station in the network sends data, a packet key is derived from the secret key and used as a key for the RC4 stream cipher for encryption. An additional checksum is appended to the packet and the packet is then XORed with the key stream and sent to destination [1]. The WEP Protocol was eminent for its security and recommended to users by router configuration tools. It was a key component in the original IEEE 802.11 standard in September 1999. Unfortunately, in 2001 flaws were recognized by a group of cryptographic researchers. After discovery of these flaws, new standards such as Wi-Fi Protected Access (WPA) and WPA2 were introduced in IEEE 802.11i Protocols. Although, the numerous defects found in WEP, it is still widely used in the wireless networks. In this project, we are investigating RC4 key strength in WEP protocols by using CrypTool 1 and 2 to simulate brute-force and FMS attacks.

Wired Equivalent Privacy (WEP)

Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key [2]. At the time that the original WEP standard was drafted, the U.S. Government's export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, manufacturers of access points implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104) as shown in the Figure 1 [3].

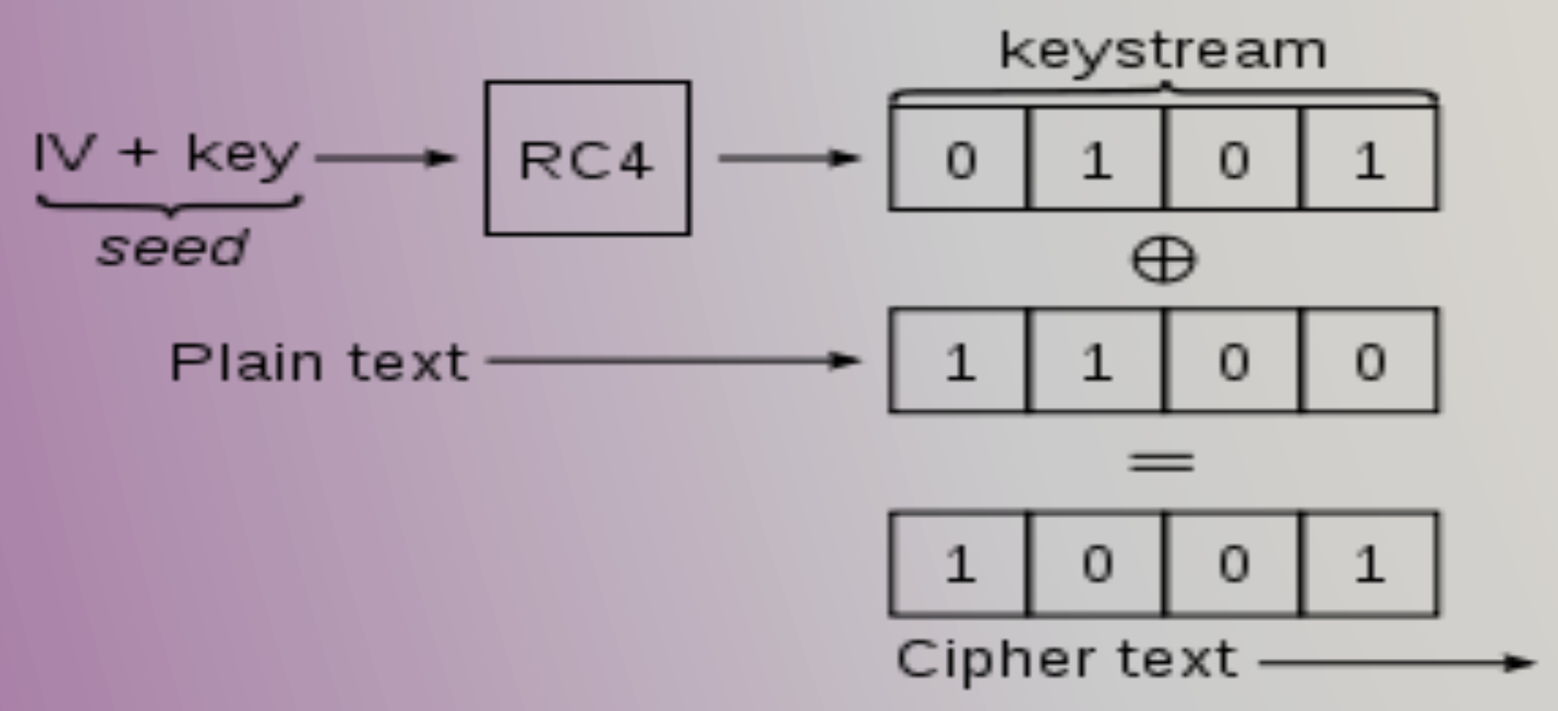


Figure 1 WEP Protocol

Attacks on WEP

WEP uses the RC4 algorithm to generate random keys to be XORed with the plaintext to create ciphertext. If the key established between the sender and receiver is weak, it will be easy for a third party to crack this key, and see the content of the data transmitted over the networks. There are two attacks that were performed in this project. First, brute-force attacks were executed, and then an FMS attack was executed. There are similarities relating the time it takes for an attacker to crack the keys using those two techniques of attacks. It was discovered that there is a linear relationship between key length and key break time in an FMS attack. On the other hand, it was also discovered that this relationship is exponential in brute-force attacks.

Weak Keys

Weak Keys in RC4	Key that does not change the S array
00 00 00… Weak (510 non-weak keys)	K(0)=0 K(1)=0
FF 01 00..Weak (254 non-weak keys)	K(2)=255 K(3)=254
FE 02 00…Weak (254 non-weak keys	. .
FD 03 00…Weak …	K(255)=2 K(254)=3
01 FF 00…Weak (254 non-weak keys)	
00 00 01…Weak (510 non-weak keys)	

Brute-Force Attack

A brute-force attack is an attack in which every possible key is tested in turn in an attempt to discover the key with which the document has been encrypted. The longer the key length, the more time it will take to discover the key. Below Figures 2 and 3 display brute-force attacks on different key lengths in the CrypTool 1 Software [5]. Followed by, a table listing the estimated times to break the key, with different key lengths derived from trials in Cryptool 1. These tests were ran on a Windows 8.1, Intel Pentium CPU 3530 @2.16GHz , with 4G RAM memory platform.

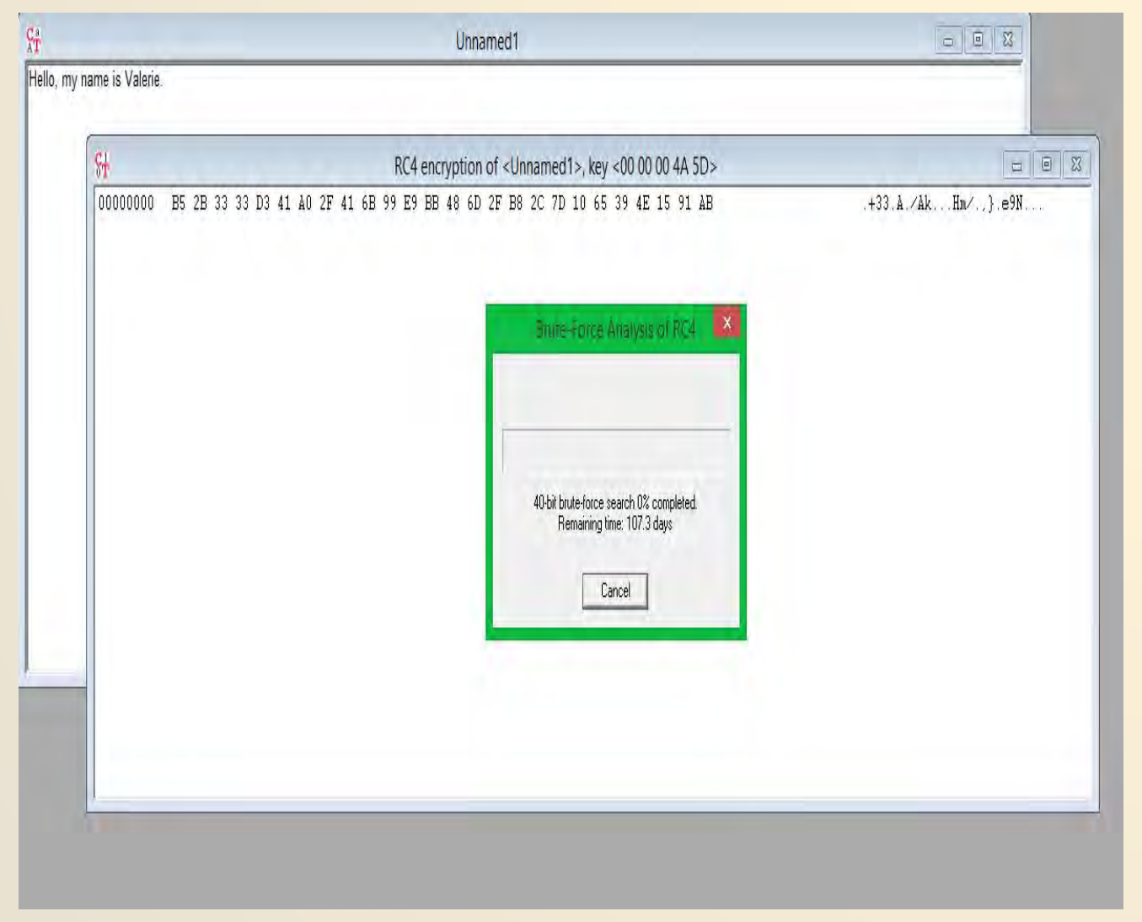


Figure 2 40-bit key brute force attack

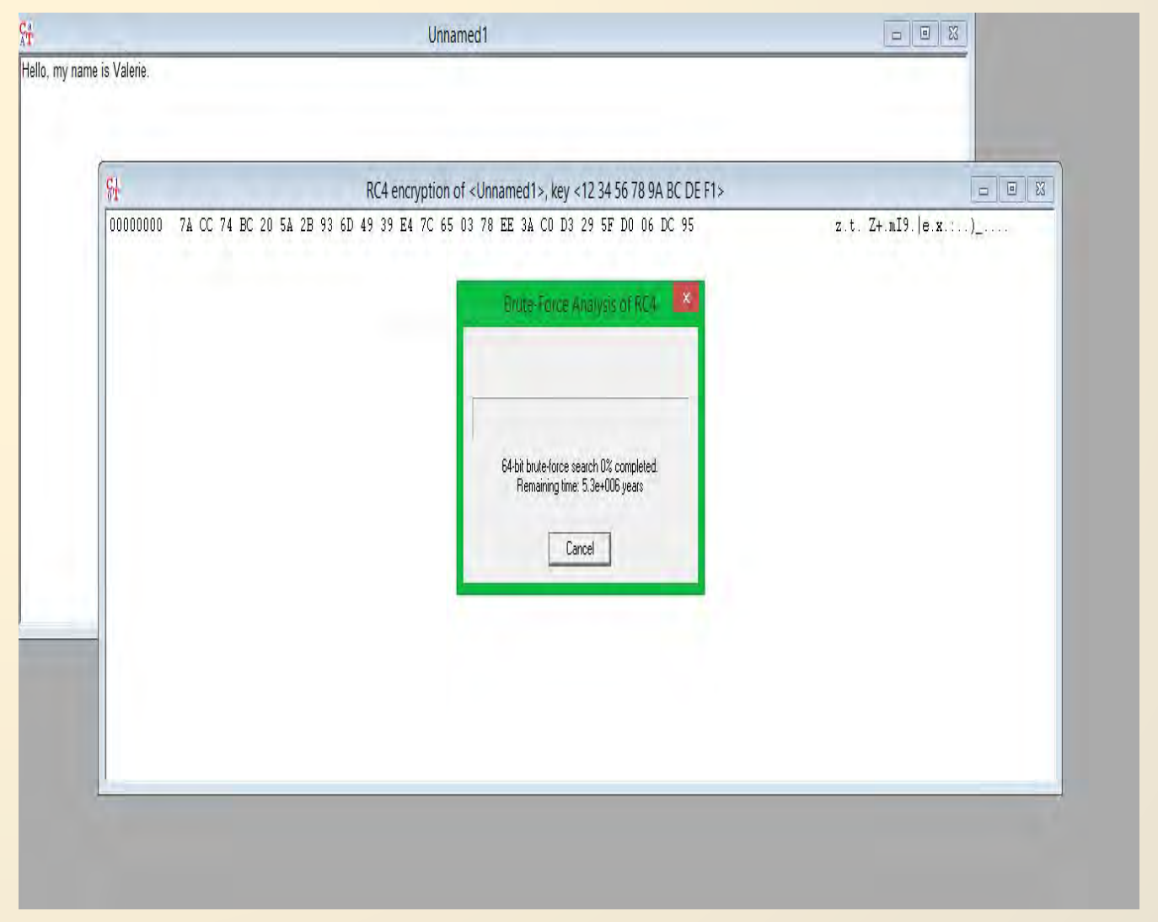


Figure 3 64-bit key brute force attack

Table 1
Estimated Key Break Time

Key Length (Bits)	Estimated Time to Break Key
8	No time
16	No time
24	1 minute 50 seconds
32	8 hours
40	106 days
48	69 years
56	2.2 *10^4 years
64	5.1*10^6 years
72	1.3*10^9 years
80	3.5*10^11 years
88	9.2*10^13 years
96	2.4*10^16 years
104	6.5*10^18 years
112	1.7*102^1 years
120	4.5*10^23 years
128	1.2*10^26 years

Fluhrer, Mantin and Shamir (FMS) Attack

This attack uses large numbers of weak keys(first 24-bits known) to discover original key with a high probability [4]. This attack set up in CrypTool 2 is shown below in Figure 4. In this attack in CrypTool 2, we captured 100,000 WEP packages as shown in Figure 5 below.

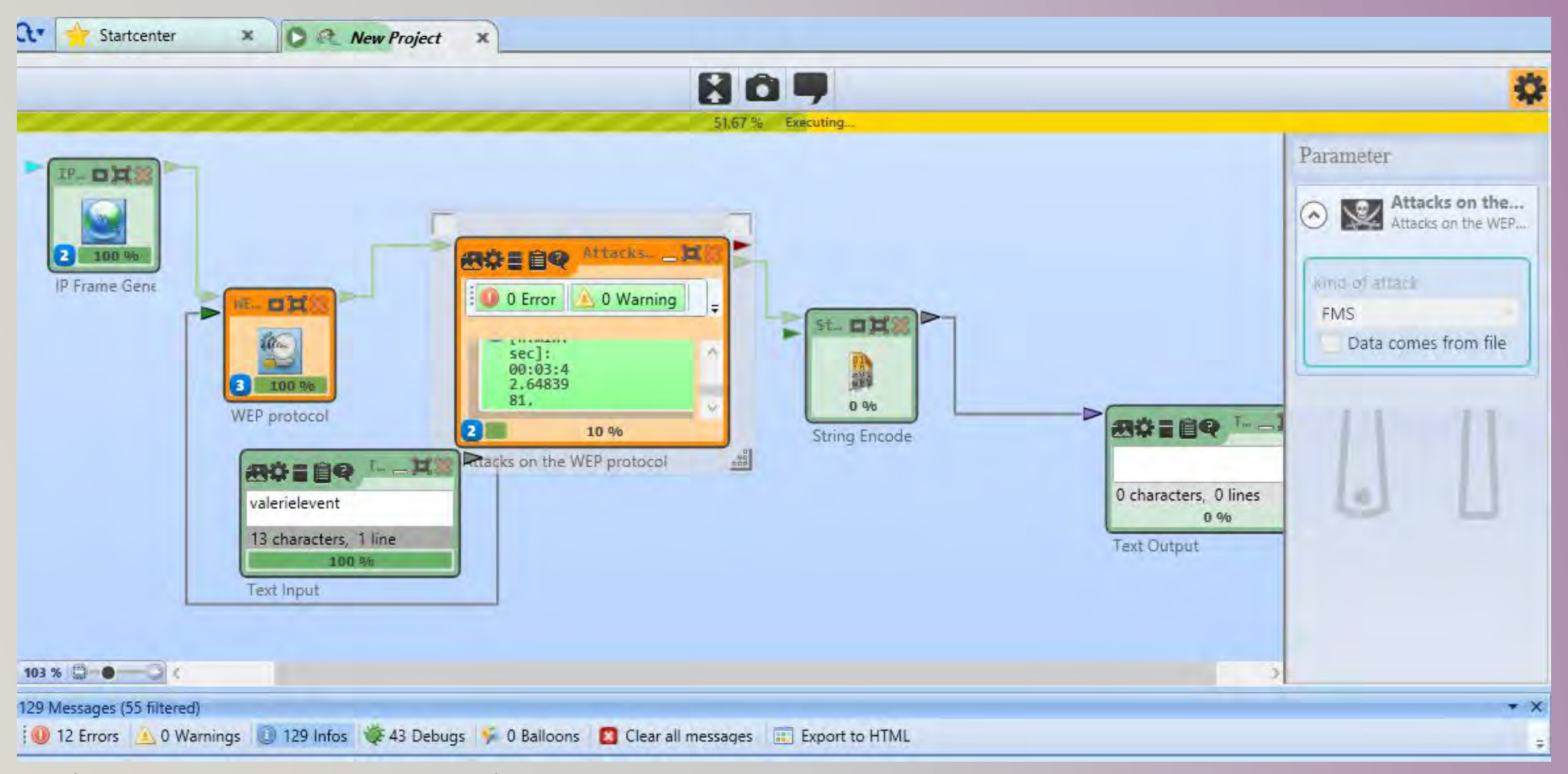
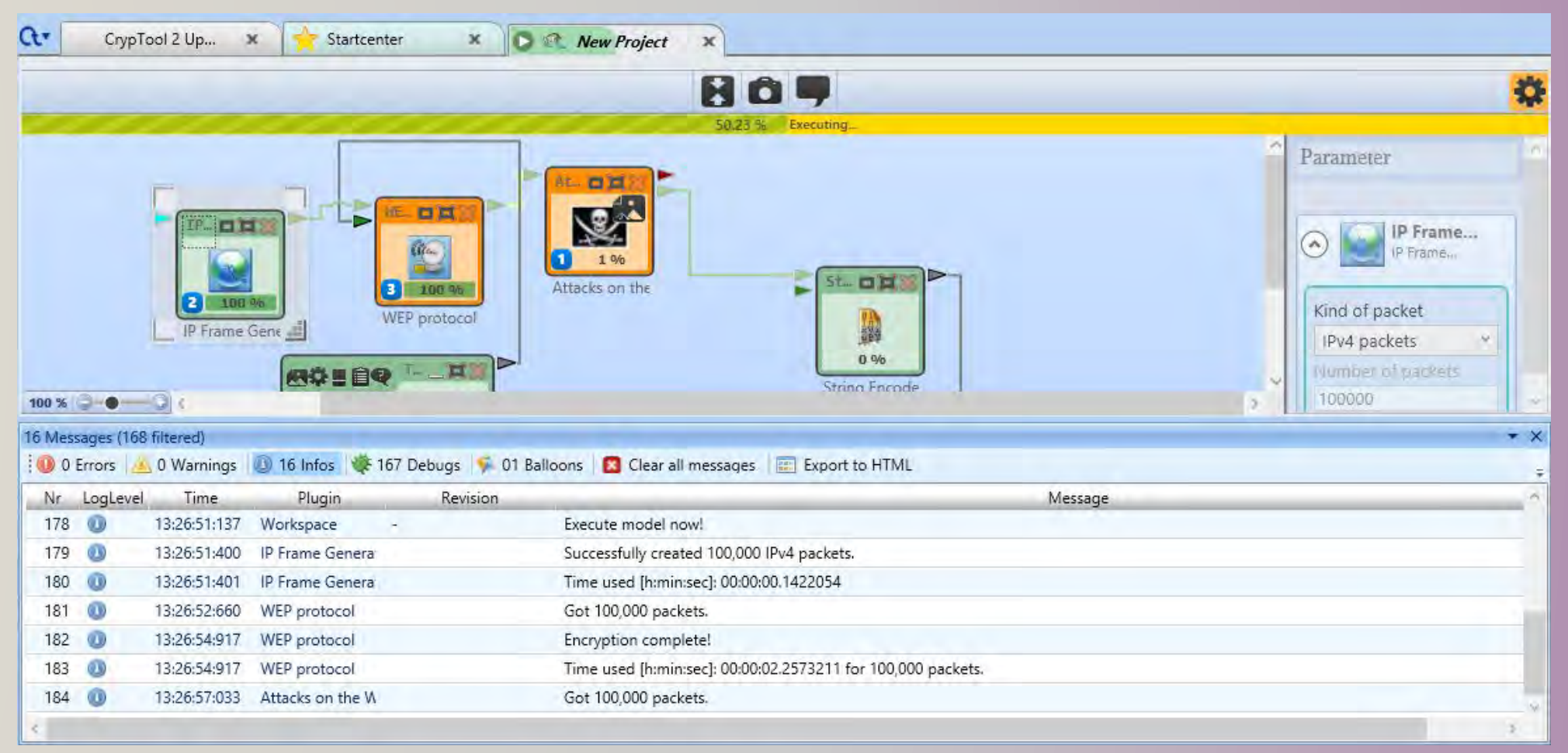


Figure 4 FMS attack setup



```
Nr   LogLevel  Time          Plugin           Revision  Message
178            13:26:51:137  Workspace        -         Execute model now!
179            13:26:51:400  IP Frame Genera            Successfully created 100,000 IPv4 packets.
180            13:26:51:401  IP Frame Genera            Time used [h:min:sec]: 00:00:00.1422054
181            13:26:52:660  WEP protocol               Got 100,000 packets.
182            13:26:54:917  WEP protocol               Encryption complete!
183            13:26:54:917  WEP protocol               Time used [h:min:sec]: 00:00:02.2573211 for 100,000 packets.
184            13:26:57:033  Attacks on the W           Got 100,000 packets.
```

Figure 5 FMS attack info

Discussion

Under the circumstances, it is very difficult to run large scale brute-force attacks. That is why, we tried FMS attacks on the weak keys because in FMS attacks time taken to break the keys has linear relationships with the key lengths. To compare the brute-force and FMS attacks, we selected minimum required key lengths (40-bits) for WEP. We ran the FMS attacks with 100, 000 packages captured. IT IS STILL RUNNING! I NEED SEQUOIA ☺

REFERENCES

1. "IEEE 802.11b Wireless Equivalent Privacy (WEP) Security," February 19, 2001, Wireless Ethernet Compatibility Alliance (WECA).
2. Robshaw, M. *Stream Ciphers*. RSA Laboratories Technical Report TR-701, July 1995. http://www.rsasecurity.com/rsalabs/index.html
3. Roos, Andrew. "Weak Keys in RC4." Netfuture. N.p., 22 Sept. 1995. Web. 31 July 2014.https://netfuture.ch/1995/09/weak-keys-in-rc4/.
4. Fluhrer, S.; Mantin, I.; Shamir, A. "Weakness in the Key Scheduling Algorithm of RC4." *Proceedings, Worshop in Selected Areas of Cryptography,* 2001.
5. www.cryptool.org

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344